

AO 106 (Rev. 04/010) Application for Search Warrant

AUTHORIZED AND APPROVED/DATE: CB 5/17/22

UNITED STATES DISTRICT COURT

FILED

WESTERN

for the
DISTRICT OF

OKLAHOMA

MAY 17 2022

In the Matter of the Search of)
 One Gigared SIM card with the)
 numbers/letters 8952020020 H6 197511148F)
 inscribed on the front)

Case No:

M-22-373-STE

CARMELITA REEDY, SHIRLEY CLERK
 U.S. DIST. COURT, WESTERN DIST. OKLA.
 BY al DEPUTY

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim.P.41(c) is (check one or more):

- ☒ evidence of the crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 371

18 U.S.C. § 2113(b)

Offense Description

Conspiracy

Bank Larceny

The application is based on these facts:

See attached Affidavit of Detective Sean Querry, Oklahoma City Police Department and Task Force Officer, which is incorporated by reference herein.

- ☐ Continued on the attached sheet(s).
☐ Delayed notice of _____ days (give exact ending date if more than 30 days) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Sean Querry
 Detective
 OCPD/USSS TFO

Sworn to before me and signed in my presence.

Date:

5/17/22

Shon T. Erwin
 Judge's signature

City and State: Oklahoma City, Oklahoma

SHON T. ERWIN, U.S. Magistrate Judge
 Printed name and title

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

A Gigared SIM card with the numbers/letters 8952020020 H6 197511148F inscribed on the front that was seized from Edgar Johan Ravelo's wallet.



ATTACHMENT B

ITEMS TO BE SEIZED

Evidence of violations of Title 18, United States Code, Sections 371 and 2113(b), among others, including:

- a. Financial records related to the fraud, however maintained, including bank account records, bank statements, deposit statements/slips, receipts, ledgers, cash receipt books, checks, checkbooks, canceled checks, check registers, withdrawal slips, wire transfers, and cashier's checks.
- b. Receipts, records, and other documents, however maintained, related to past and future travel.
- c. Evidence of travel history, however maintained, including global positioning system location, that provides information on dates, times, and/or location of each subject device.
- d. Directories and/or contacts list, calendars, text messages, multi-media messages, e-mail messages, call logs, photographs, and videos.
- e. Evidence of conspiracy, including communications with phones numbers associated with other individuals or groups involved in criminal activity.
- f. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- g. Evidence of user attribution showing who used or owned the subject devices at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Sean Query, a Detective with the Oklahoma City Police Department, and a Task Force Officer with the United States Secret Service, being duly sworn, hereby depose and state as follows:

Introduction

1. I have been an Oklahoma City Police Department officer since May 2000 and have been assigned to the White-Collar Crimes Unit since 2017. I am also a member of the United States Secret Service Cyber Crimes Task Force (the “task force”). As a Detective and a member of the task force, I have conducted and assisted other agents with investigations involving criminal violations of Title 18 of the United States Code, including mail fraud, bank fraud, wire fraud, computer fraud, bank theft, and identity theft.

2. I am experienced in executing search warrants and debriefing defendants, witnesses and other persons who have knowledge of specific crimes in violation of the above-mentioned title of the United States Code.

3. Based on my training and experience, I know that individuals who commit financial crimes maintain books, records, receipts, notes, ledgers, bank records, wire transfer receipts, and other items relating to their fraud and to their clients and associates.

4. Based on my training and experience, I know that individuals who commit financial crimes often maintain records of their correspondence and transactions with their clients and associates. These records may be in the form of written notes and

correspondence, receipts, negotiated instruments, bank statements, and other records. Records of this kind are often stored on computer media, including on cellular phones.

5. Based on my training and experience, I know that individuals who commit financial crimes commonly maintain contact information of their clients and associates.

6. Based on my training and experience, I know that individuals who commit financial crimes utilize cellular phones to maintain contact with clients and associates. Furthermore, based on my training and experience, I know that individuals who commit financial crimes often utilize e-mails, text messages, and other communication software to communicate with their clients and associates.

7. Based on my training and experience, I know that individuals who commit financial crimes use electronic devices, including cellular phones, computers, USB drives, and SIM cards to maintain records related to the receipt and disposition of the proceeds derived from the fraudulent conduct.

8. I present this affidavit in support of an application for a warrant to search a Gigared SIM card (the "subject device") located at the United States Secret Service computer lab, 210 Park Ave, Suite 1100, Oklahoma City, Oklahoma. This affidavit sets forth facts to establish probable cause to believe that evidence, fruits, and instrumentalities of illegal activity in violation of, among other statutes, 18 U.S.C. § 371 (conspiracy) and 18 U.S.C. § 2113(b) (bank larceny) are currently located on the subject device. This affidavit further provides probable cause to believe that Chevalier Jesus Martinez, Edgar Johan Ravelo, Wilfredo Alberto Lezama-Garcia, and Clever Andres Medina-Martinez have committed the federal offenses listed above.

9. Since I am submitting this affidavit for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause that evidence, fruits, and instrumentalities of violations of the statutes described above are presently located on the subject device. This affidavit is based on my own personal knowledge, as well as information provided by records, databases, and other law enforcement officers.

ATM Jackpotting

10. ATM “jackpotting” is a relatively new scheme where criminals install malicious software and/or hardware at ATMs that forces the machines to spit out large amounts of cash on demand. Jackpotting often targets financial institutions that operate stand-alone ATMs located inside big-box retailers, gas stations, and convenience stores.

11. To carry out a jackpotting attack, criminals first gain physical access to the cash machine. They then install malware or specialized electronics — often a combination of both — to control the operations of the ATM. This physical access does not need to include access to the inside of the ATM itself but can also include a slight variation of the scheme known as a “man-in-the-middle” attack.

12. With a man-in-the-middle attack, criminals place a device between the ATM and its wireless communication box, altering communications between the ATM and the card processing service. This device and/or software allows the criminals to force the ATM to receive an approved withdrawal transaction and dispense cash.

13. Criminals often target multiple ATMs in the span of a couple days before fleeing the area with little risk of being caught due to the difficulty of identifying and responding to a jackpotting attack in progress. Jackpotting attacks are often first detected when the financial institution or ATM service provider conducts a reconciliation of the targeted ATM.

Probable Cause

14. Since September 2021, TransFund has been the victim of coordinated ATM jackpotting attacks in Oklahoma City and other areas throughout the region. TransFund is a subsidiary of Bank of Oklahoma, and it operates a large ATM network throughout the Oklahoma City area. At all times material to this investigation, Bank of Oklahoma was a financial institution, the accounts and deposits of which were insured by the Federal Deposit Insurance Corporation. As of today, over 100 jackpotting attacks have caused over \$7 million in losses to Bank of Oklahoma.

15. On January 23, 2022, at least two individuals conducted a successful jackpotting attack at a TransFund ATM located inside an OnCue convenience store at Memorial Road and Western Avenue in Oklahoma City. Video footage showed the individuals inserting a magnetic stripe card into the ATM and obtaining a receipt moments before the physical intrusion into the ATM. TransFund identified the magnetic stripe card (XXXX XXXX XXXX 1421) that was swiped prior to the attack and then issued an alert for that card number. Based on my review of the surveillance footage, I believe the two individuals involved in this jackpotting attack were Chevalier Jesus Martinez and Clever Andres Medina-Martinez. The footage shows Chevalier Jesus

Martinez enter the store and insert the card into the ATM. Clever Andres Medina-Martinez then enters the store, opens the top portion of the ATM, and tampers with the ATM's computer. Chevalier Jesus Martinez returns to the ATM and appears to place cash being dispensed from the ATM into the fanny pack he is wearing around his waist. This January 23, 2022, jackpotting attack caused a loss of \$22,400 to Bank of Oklahoma. Bank of Oklahoma ran a historical search on the card ending in 1421 and discovered that it had been used at several other ATMs just prior to confirmed jackpotting attacks.

16. On April 14, 2022, TransFund received a notification that at approximately 11:59 a.m., the card ending in 1421 had been inserted into a TransFund ATM located inside an OnCue convenience store in Del City, Oklahoma. Surveillance footage showed two subjects, later identified as Chevalier Jesus Martinez and Clever Andres Medina-Martinez, entered the store around 11:59 a.m. and went directly to the ATM and inserted a card. Clever Andres Medina-Martinez was wearing a red St. Louis Cardinals ballcap with a sticker on the bill's exterior and grey sweatpants. Chevalier Jesus Martinez was wearing the same shirt, jeans, and shoes that he was arrested in later that date. While these two subjects were at the ATM, another subject, later identified as Edgar Johan Ravelo, was inside the OnCue conducting surveillance. The subjects left the store without completing a jackpotting attack. At approximately 12:45 p.m., task force officers responded to the Del City OnCue but did not locate any of the subjects.

17. At approximately 3:00 p.m. on that same date, TransFund received a notification that the card ending in 1421 had been inserted into a TransFund ATM located inside an OnCue convenience store at Memorial Road and Western Avenue in Oklahoma

City. Surveillance footage shows Chevalier Jesus Martinez and Wilfredo Lezama-Garcia approach the ATM at approximately 2:59 p.m., which is the same time that TransFund confirmed the card ending in 1421 was first used at that ATM. Chevalier Jesus Martinez inserts the card and then appears to tamper with the exterior of the ATM before unlocking the top portion of the ATM, which provided access to the ATM's computer. Wilfredo Lezama-Garcia stands immediately to the right of Chevalier Jesus Martinez, blocking the line of sight of the cashiers. These two subjects then leave the store.

18. Clever Andres Medina-Martinez then enters the OnCue wearing a blue shirt, red wig, and dark fanny pack, while carrying a keyboard. He immediately approaches the ATM, slides the top portion of the machine out, and appears to connect the keyboard to the ATM's computer. TransFund confirmed that this ATM went offline at approximately 3:21 p.m. After working inside the ATM for several minutes, Clever Andres Medina-Martinez removes the keyboard, closes the top portion of the ATM, and then leaves the store. During this time, Edgar Johan Ravelo is seen in front of the OnCue conducting surveillance and briefly speaking with Chevalier Jesus Martinez. At approximately 4:36 p.m., Clever Andres Medina-Martinez enters the OnCue, approaches the ATM, and slides the top portion out. He appears to remove something from inside the ATM before closing it up and leaving the store. TransFund confirmed this ATM went back online at approximately 4:38 p.m. and was fully operational at 4:39 p.m.

19. Taskforce officers saw Clever Andres Medina-Martinez leave the OnCue and get into the front passenger seat of a Nissan Altima at approximately 4:40 p.m. Officers immediately stopped the Nissan Altima, which was being driven by Wilfredo

Lezama-Garcia. Edgar Ravelo was sitting in the back seat. Officers removed the three subjects and patted them down. Clever Andres Medina-Martinez was holding a cellular phone when he was removed from the Nissan Altima. Officers seized two SIM cards, including the subject device described in Attachment A, from Edgar Johan Ravelo's wallet, which was in his back pocket when they removed him from the Nissan Altima. Officers searched the interior of the Nissan Altima and seized a dark fanny pack full of tools and a SanDisk USB drive from the floorboard of the front passenger side. Officers also seized a laptop, three cellular phones, and a pocket-sized keyboard from the interior of the Nissan Altima. Additionally, officers seized several hats and articles of clothing, including the red wig and blue shirt that Clever Medina-Martinez was wearing when he opened the ATM.

20. The Nissan Altima is registered to Wilfredo Lezama-Garcia, who purchased it on December 28, 2021. According to documents found inside the Nissan Altima, it appears that it has been driven approximately 23,350 miles between December 28, 2021, and March 9, 2022.

21. Officers arrested the three subjects who were inside the Nissan Altima for various state charges, including conspiracy and violations of the Oklahoma Computer Crimes Act, and booked them into the Oklahoma County jail. Chevalier Jesus Martinez was arrested as he attempted to walk away from the store. Chevalier Jesus Martinez was holding a cellular phone when he was arrested. Officers searched Chevalier Jesus Martinez and found the card ending in 1421 and several hundred dollars of cash inside

his back pocket. He was arrested on the same charges and booked into the Oklahoma County jail.

22. Clever Andres Medina-Martinez waived *Miranda* and agreed to speak with the officers. He admitted to wearing the disguise into the OnCue and opening the ATM machine. He stated that he has known the other three suspects whom he identified as Chevalier, Wilfredo, and Johan, since he lived in Venezuela years ago. He explained that he was doing what “they” had told him to do but would not elaborate on who exactly told him what to do. Clever Andres Medina-Martinez admitted that he had opened the machine and plugged in a “Bluetooth” and then “hit some keys on the keyboard.” Although he admitted he knew what he was doing was wrong, he denied being paid any money to do this and would not elaborate as to how or why he became involved.

23. On April 15, 2022, United States Magistrate Judge Amanda Maxfield Green signed a criminal complaint authorizing the arrest of these subjects. *See United States v. Lezama-Garcia, et al.*, M-22-280-AMG. Following a preliminary hearing for all four defendants on May 4, 2022, United States Magistrate Judge Suzanne Mitchell found probable cause that each of the defendants had committed at least one of the offenses alleged in the complaint. *See* Doc. Nos. 52 – 53, 55, 58.

24. Bank of Oklahoma confirmed there was \$85,020 in the TransFund ATM located at the OnCue on Memorial Road and Western Avenue during the time of the attempted jackpotting on April 14, 2022.

Technical Terms

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Cellular telephone*: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A cellular telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. *GPS*: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

26. Based on my knowledge, training, and experience, I know that the subject device described in Attachment A has the capabilities that allows it to serve as a cellular telephone and/or GPS navigation device. In my training and experience, examining data

stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Electronic Storage and Forensic Analysis

27. Based on my knowledge, training, and experience, I know that electronic devices such as the subject device can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant, but also forensic evidence that establishes how the subject device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the subject device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

29. *Manner of execution.* Because this warrant only seeks permission to examine the subject device that is already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

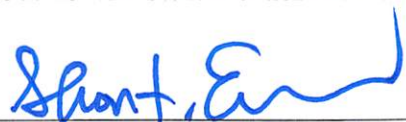
30. Based on the above information, I respectfully submit there is probable cause to believe the subject device described in Attachment A that is located at 210 Park Ave, Suite 1100 in Oklahoma City, Oklahoma, contains evidence of violations of 18 U.S.C. §§ 371 and 2113(b), among others. The items listed in Attachment B are evidence of these crimes, contraband, fruits of these crimes, or property that is or has been used as the means of committing the foregoing offenses.

Therefore, I respectfully request that a search warrant be issued, authorizing the search of the subject device described in Attachment A, and the seizure of the items listed in Attachment B.



Sean Querry
Oklahoma City Police Department
USSS Task Force Officer

Subscribed to and sworn before me on May 17, 2022.



SHON T. ERWIN
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

A Gigared SIM card with the numbers/letters 8952020020 H6 197511148F inscribed on the front that was seized from Edgar Johan Ravelo's wallet.



ATTACHMENT B

ITEMS TO BE SEIZED

Evidence of violations of Title 18, United States Code, Sections 371 and 2113(b), among others, including:

- a. Financial records related to the fraud, however maintained, including bank account records, bank statements, deposit statements/slips, receipts, ledgers, cash receipt books, checks, checkbooks, canceled checks, check registers, withdrawal slips, wire transfers, and cashier's checks.
- b. Receipts, records, and other documents, however maintained, related to past and future travel.
- c. Evidence of travel history, however maintained, including global positioning system location, that provides information on dates, times, and/or location of each subject device.
- d. Directories and/or contacts list, calendars, text messages, multi-media messages, e-mail messages, call logs, photographs, and videos.
- e. Evidence of conspiracy, including communications with phones numbers associated with other individuals or groups involved in criminal activity.
- f. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- g. Evidence of user attribution showing who used or owned the subject devices at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.